**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF OKLAHOMA**

| | | |
|---|---|---|
| ROBERT LEGG, individually and on behalf Of himself and all others similarly situated, | ) | |
| Plaintiff, | ) | |
| v. | ) | CIV-21-655-D |
| LEADERS LIFE INSURANCE COMPANY, | ) | |
| Defendant. | ) | |

**ORDER**

Before the Court is Defendant Leaders Life Insurance Company's Motion to Dismiss Plaintiff's First Amended Complaint [Doc. No. 11]. The motion seeks dismissal of Plaintiff's claims pursuant to Fed.R.Civ.P 12(b)(1) and 12(b)(6), or in the alternative an order striking certain allegations pursuant to Fed.R.Civ.P. 12(f). Plaintiff has responded in opposition [Doc. No. 12] and Defendant has replied [Doc. No. 13]. As explained below, Plaintiff has failed to plausbily plead that he has suffered an injury in fact and he therefore lacks standing to pursue his claims.

**BACKGROUND**

This putative class action involves a data breach at Defendant Leaders Life Insurance Company. Plaintiff, a customer of Leaders Life, alleges that in late November 2020, a third-party intentionally accessed and removed folders containing personal identifying information from Leaders Life's computer systems. *Id.* at ¶ 19. Among the information allegedly obtained was customer names, dates of birth, social security numbers, and tax identification numbers. *Id.* at ¶¶ 5, 21. In June 2021, nearly seven months

after the data breach, Leaders Life sent Plaintiff a letter informing him of the cyberattack. The letter explained that "certain folders on our system may have been accessed or removed from our systems without authorization," "one or more of the potentially impacted folders included protected information related to individuals," and "there is no indication that your specific information was accessed or misused." *Id.* at ¶ 21. Nevertheless, Plaintiff alleges that his personal identifying information is "now in the hands of cybercriminals who will use their PII [personal identifying information] to commit fraud and identity theft." *Id.* at ¶ 23.

Plaintiff brings five claims on behalf of himself and a putative class against Leaders Life as a result of the data breach. First, he asserts that Leaders Life acted negligently in failing to protect Plaintiff's information or provide adequate data security. Second, he asserts that Leaders Life breached an implied contract obligating it to provide adequate data security. Relatedly, his third claim asserts that Leaders Life breached an implied covenant of good faith and fair dealing when it engaged in acts or omissions that have been declared to be unfair trade practices. Fourth, he asserts that Leaders Life engaged in deceptive practices in violation of the Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-301.[1] Last, Plaintiff asserts a claim for declaratory and injunctive relief based on Leaders Life's past failure to comply with its contractual obligations and duties of care and inability to prevent future cyberattacks.

[1] This particular claim is brought only on behalf of Plaintiff and a proposed subclass of Maryland customers.

Crucially, Plaintiff does not allege that he or any other class member has been the victim of identity theft or fraud. Instead, he describes his injuries as including "an imminent, immediate, and continuing risk of harm from identity theft and fraud." *Id.* at ¶ 72. Plaintiff further alleges that the "threat of fraud and identity theft" has caused "increased emotional distress and anxiety" as well as a loss of time and money spent addressing and attempting to mitigate the consequences of the data breach. *Id.* at ¶ 75.

Defendant moves to dismiss under Fed.R.Civ.P. 12(b)(1), arguing that Plaintiff has failed to plead an injury in fact and therefore lacks standing to bring his claims.[2]

**STANDARD OF DECISION**

Federal courts are courts of limited jurisdiction. Article III of the Constitution "confines the federal judicial power to the resolution of 'Cases' and 'Controversies.'" *TransUnion LLC v. Ramirez*, __ U.S. __, 141 S. Ct. 2190, 2203 (2021). "For there to be a case or controversy under Article III, the plaintiff must have a personal stake in the case—in other words, standing." *Id.* (internal quotation marks omitted). Constitutional standing requires a plaintiff to show that he "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

[2] Defendant also seeks dismissal under Fed.R.Civ.P. 12(b)(6) and seeks to strike certain allegations under Fed.R.Civ.P. 12(f). It is not, however, appropriate to address these arguments where the Court lacks subject matter jurisdiction over the case. *See D.L. v. Unified Sch. Dist. No.* 497, 392 F.3d 1223, 1229 (10th Cir. 2004) (explaining that "a determination that the district court lacked jurisdiction over a claim moots any other challenge to the claim, including a different jurisdictional challenge.").

The first element – injury in fact – requires a plaintiff to show that he "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). A "concrete" injury may include tangible or intangible harms, so long as they "actually exist" and are "'real,' and not 'abstract.'" *Id.* A real, existing injury is a prerequisite to federal jurisdiction because "federal courts do not adjudicate hypothetical or abstract disputes" nor do they "exercise general legal oversight…of private entities." *TransUnion*, 141 S. Ct. at 2190.

As the party invoking federal jurisdiction, the plaintiff bears the burden of establishing the three elements for standing. *Spokeo, Inc.*, 578 U.S. at 338. When considering standing in the context of a motion to dismiss, the Court "must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *S. Utah Wilderness All. v. Palma*, 707 F.3d 1143, 1152 (10th Cir. 2013) (quotation omitted). But even "at the pleading stage, the plaintiff must 'clearly...allege facts demonstrating' each element." *Spokeo*, 578 U.S. at 338 (quotation omitted). Further, in a putative class action, the named representative must personally allege that he has standing to sue. *See Warth v. Seldin*, 422 U.S. 490, 502 (1975); *Big Elk v. Bd. of Cty. Comm'rs of Osage Cty.*, 3 F. App'x 802, 807 (10th Cir. 2001). "And standing is not dispensed in gross; rather, plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion*, 141 S.Ct. at 2208.

## DISCUSSION

Data breaches of the type alleged here are becoming ubiquitous in our increasingly digital society and, unsurprisingly, are also becoming the subject of a growing amount of litigation. But does the mere fact that a data breach occurred necessarily mean that a customer has suffered a concrete injury, or is something more required? The Tenth Circuit has not had occasion to resolve this precise issue, but several other circuits have. After reviewing these decisions, the Court will summarize two relevant Supreme Court opinions – *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), and *TransUnion*, 141 S. Ct. at 2190 – before analyzing the allegations in this case.

### A. Relevant Circuit Court Decisions

The Fourth, Sixth, Seventh, Ninth, and District of Columbia Circuits have all found standing for a plaintiff who alleged he was the victim of a data breach. The earliest case is *Remijas v. Neiman Marcus, LLC*, 794 F.3d 688, 690 (7th Cir. 2015), a class action which involved the unauthorized exposure of 350,000 credit card numbers from the defendant's database and fraudulent charges on 9,200 of the cards. The Seventh Circuit held that even those plaintiffs who had not experienced fraudulent charges had standing to pursue their claims because their risk of future injury was substantial. *Id.* at 693. The court reasoned that "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." *Id.* (quoting *Clapper*, 568 U.S. at 410).[3]

[3] The Seventh Circuit reached a similar result in *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016). There, the Court found that the plaintiffs' present injuries,

Similarly, in *Galaria v. Nationwide Mut. Ins. Co*., 663 F. App'x 384, 388 (6th Cir. 2016), the Sixth Circuit held that the plaintiffs had standing to bring claims against an insurance company following a cyberattack that exposed personal identifying information. In reaching this conclusion, the Court explained that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Id.* at 388. Like in *Remijas*, the complaint in *Galaria* included an allegation that the named class representative had already been the victim of attempted fraud. *Id.* at 387.

The District of Columbia Circuit likewise found standing in a data breach case because "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Attias v. Carefirst, Inc*., 865 F.3d 620, 629 (D.C. Cir. 2017). Again, however, *Attias* included an allegation that two of the named plaintiffs had suffered identity theft as a result of the breach. *Id.* at 626 n.2.

The Fourth Circuit similarly found that the plaintiffs had standing to bring claims following a data breach where the plaintiffs alleged that they had "already suffered actual harm in the form of identity theft and credit card fraud." *Hutton v. Nat'l Bd. of Examiners*

---

which included fraudulent charges on a credit card for one of the named representatives but not the other, and the future risk of fraud were sufficient to confer standing. An earlier Seventh Circuit decision, *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007), explicitly held that the plaintiffs had standing to bring claims based on a data breach even though no misuse had occurred, but that case was decided prior to the Supreme Court's decision in *Clapper*, 568 U.S. at 398, discussed *infra*.

*in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018).[4] But the Fourth Circuit also made clear that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Id.* at 621.

Finally, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) and *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018), the Ninth Circuit held that the plaintiffs had standing to bring claims based on a data breach because it placed them at imminent risk of identity theft. Both cases included allegations that at least one plaintiff had experienced some sort of misuse of his personal data following the breach. *Krottner*, 628 F.3d at 1142; *In re Zappos.com*, 888 F.3d at 1027.

Notably, all of the circuit court cases "conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse." *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021). Conversely, where no allegations of misuse are present, circuit courts have generally declined to find standing. In *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011), the defendant suffered a security breach that may have allowed a third-party to read and copy data containing names, addresses, social security numbers, dates of birth, and bank account information of its customers' employees. The Third Circuit dismissed the case at the pleading stage, concluding that "[i]n data breach cases where no misuse is alleged…there

[4] In *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017), the Fourth Circuit declined to find standing based on a threat of future injury following the theft of a laptop containing personal identifying information because the information had not been misused or intentionally targeted. The Fourth Circuit distinguished *Hutton* from *Beck* by noting that the *Hutton* plaintiffs alleged actual misuse of the data. *Hutton*, 892 F.3d at 621-622.

has been no injury." *Id.* at 45. The Third Circuit reasoned that the plaintiffs' allegations of "hypothetical, future injury" were insufficient because they

> rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.

*Id.* at 42.

The Eighth Circuit addressed standing in the context of a data breach in *In re SuperValu, Inc*., 870 F.3d 763, 766 (8th Cir. 2017). Like the instant case, the plaintiffs in *SuperValu* argued that they "sufficiently alleged an injury in fact because the theft of their [credit] Card Information due to the data breaches at defendants' stores creates the risk that they will suffer identity theft in the future." *Id.* at 768-769. The Eighth Circuit dismissed the case for lack of standing at the pleading stage because allegations that "illicit websites are selling their Card Information to counterfeiters and fraudsters" were "speculative" and "fail[ed] to allege any injury 'to the plaintiff[s].'" *Id.* at 770 (quotation omitted). Further, the Eight Circuit held that the plaintiffs had not demonstrated a substantial risk of future identity theft because the report they relied on – a 2007 GAO report that is also cited in Plaintiff's Amended Complaint – does "not plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud." *Id.* at 771.

More recently, the Eleventh Circuit addressed standing in the context of a data breach in *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).

The plaintiff in *Tsao* alleged that the defendant had been the target of a cyberattack, his credit card information may have been accessed in the attack, and that he cancelled his credit cards as a result. The Eleventh Circuit dismissed for lack of standing because conclusory allegations of a continuing risk of identity theft "without specific evidence of some misuse of class members' data" does not establish a concrete injury. *Id.* at 1343-1344.[5]

Last, the Second Circuit dismissed a data breach case for lack of standing in *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021). There, the defendant's employee accidentally sent an email that contained personal identifying information of current and former employees. *Id.* at 298. The parties reached a settlement before the defendant's motion to dismiss was resolved, but the district court dismissed the case for lack of standing. *Id.* at 298-299. The Second Circuit affirmed, holding that a mere increased risk of identity theft can be a concrete injury, but that the allegations in this case were insufficient because the data was not intentionally targeted or misused in anyway. *Id.* at 303-304.[6]

---

[5] Four months after *Tsao*, the Eleventh Circuit decided *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021), cert. denied sub nom. *Huang v. Spector*, No. 21-336, 2021 WL 5043620 (U.S. Nov. 1, 2021), which involved a data breach that exposed personal identifying information. Citing to *Tsao*, the Eleventh Circuit found that the plaintiffs had suffered a concrete injury, explaining that "the allegations of some Plaintiffs that they have suffered injuries resulting from actual identity theft support the sufficiency of all Plaintiffs' allegations that they face a risk of identity theft." *Id.* at 1263.

[6] In a prior, unpublished decision, the Second Circuit dismissed a data breach case for lack of standing at the pleading stage even though there were allegations of misuse. *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017). The plaintiff alleged that her credit card information was stolen in a data breach, fraudulent charges were made, and she faces a future risk of identity theft. The Second Circuit held that these allegations did not

**B. Relevant Supreme Court Decisions**

Most cases declining to find standing in the data breach context rely on *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013). *Clapper* involved a group of plaintiffs whose work allegedly required them to engage in sensitive communications that might be subject to surveillance under a federal statute. *Id.* at 406. The Supreme Court held that the plaintiffs did not have standing to enjoin the enforcement of the statute because a "'threatened injury must be *certainly impending* to constitute injury in fact,'" and "'[a]llegations of *possible* future injury' are not sufficient." *Id.* at 409 (quotation omitted) (alterations in original). Under this standard, an "objectively reasonable likelihood" that a future injury will come to pass is inadequate. *Id.* at 410. Further, a plaintiff cannot establish an imminent future injury for standing purposes when they "rel[y] on a highly attenuated chain of possibilities" or "speculation about the decisions of independent actors." *Id.* at 410-414.

*Clapper* also held that measures the plaintiffs took to protect themselves from possible, future surveillance did not confer a present injury in fact. *Id.* at 415-416. On this point, the Supreme Court explained that

> Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.
>
> If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.

---

establish a concrete injury because the plaintiff was never asked to pay for any fraudulent charges and her stolen credit card was promptly cancelled. *Id*. at 90.

*Id.* at 416. In sum, the Supreme Court held "that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm." *Id.* at 422.

Relying on the risk of a future injury to show standing was further curtailed in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), which postdates all of the circuit court opinions discussed above. There, a class of plaintiffs sued TransUnion under the Fair Credit Report Act for maintaining inaccurate credit reports. *Id.* at 2200. For a subset of plaintiffs, TransUnion actually provided the inaccurate reports to third-party businesses. *Id.* For the remaining plaintiffs, TransUnion only maintained the inaccurate credit reports in their internal system and never provided the information to third parties. *Id.* Those plaintiffs, the Supreme Court held, did not have standing to sue for a statutory violation of the Fair Credit Reporting Act because "the mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.* at 2210.[7]

The Supreme Court also considered whether the mere risk of future disclosure of the inaccurate credit reports constitutes a separate concrete injury. *Id.* Citing to *Clapper*, the Supreme Court explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id.* But where a plaintiff brings "a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a

[7] *TransUnion* was decided following a jury verdict for the plaintiffs. 141 S.Ct. at 2201.

concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm." *Id.* at 2210-2211.

Applying these principles, the Supreme Court held that the plaintiffs whose reports were undisclosed did not suffer a concrete injury because they "did not demonstrate that the risk of future harm materialized" and they were not "independently harmed by their exposure to the risk itself." *Id.* at 2211. The Supreme Court further explained that in addition to the "fundamental problem with their argument based on the risk of future harm, the plaintiffs did not factually establish a sufficient risk of future harm to support Article III standing." *Id.* at 2211-2212. Although the plaintiffs "claimed that TransUnion could have divulged their misleading credit information to a third party at any moment," the Supreme Court held that the plaintiffs had not demonstrated a sufficient likelihood that the inaccurate information would be released. *Id.* at 2212.

The Supreme Court then reiterated that "the risk of future harm on its own does not support Article III standing for the plaintiffs' damages claim." *Id.* at 2213. Given the holding in *TransUnion*, it is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft following a data breach is still good law, at least with respect to a claim for damages.

**C. Analysis of Plaintiff's Allegations**

In this action, Plaintiff seeks injunctive relief and damages based not on any actual fraud or identity theft that occurred as a result of the data breach, but on the risk that fraud or identity theft may occur in the future. But as explained in *TransUnion*, the risk of future harm alone cannot support standing for a damages claim. *Id.*

As to his request for injunctive relief, in order to show a concrete injury, Plaintiff must plausibly plead that the risk of future harm as a result of the data breach is imminent, meaning it is "certainly impending." *Clapper*, 568 U.S. at 409. Unlike the majority of circuit court cases that have found a concrete injury following a data breach, Plaintiff here does not allege that any misuse of the data has occurred. The closest Plaintiff comes to alleging misuse is a statement that there has been a "dramatic increase in the amount and frequency of phishing emails he has been receiving over the last few months." Compl. ¶ 53. But the receipt of phishing emails, while perhaps "consistent with" data misuse, does not "plausibly suggest" that any actual misuse of Plaintiff's personal identifying information has occurred. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007).

Without any actual misuse of the data, Plaintiff relies on reports that describe the general risks of identity theft, explain how personal information can be sold on illicit internet sites, and identify other data breaches. But "[t]hese reports do nothing to clarify the risks to the plaintiffs in this case." *Tsao*, 986 F.3d at 1343. Further, according to Plaintiff's own allegations, the likelihood of identity theft occurring is relatively small: "nearly one out of four data breach notification recipients *becomes* a victim of identity fraud." Compl. ¶ 27 (emphasis in original). Assuming the truth of this allegation, a less than 25% chance that some form of identity fraud could occur at some unknown, future date can hardly be described as "certainly impending" or a "substantial risk." *See TransUnion*, 141 S.Ct. at 2210; *Clapper*, 568 U.S. at 415 n.5. This is particularly true given that identity theft or fraud will only occur if unknown third parties undertake a series of acts, including the comprehension and organization of the stolen data, the posting of the

data for sale, the consummation of a transaction, and then the actual use of the data to make unauthorized purchases or open fraudulent accounts. A future risk of injury that relies on this sort of "speculation about the decisions of independent actors" is not sufficient to establish a concrete injury. *Clapper*, 568 U.S. at 410-414; *see also Reilly*, 664 F.3d at 42 ("Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").

At best, then, Plaintiff's allegations lead to a plausible inference that at some unknown time in the future, some of the putative class members *may* be the victim of identity theft or fraud. Even accepting as true Plaintiff's allegations about the nature of the breach – that it was an intentional attack by cybercriminals – Plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach. This is not sufficient to confer standing.[8] *Clapper*, 568 U.S. at 409.

No doubt wary that his allegations of future harm are insufficient to confer standing, Plaintiff additionally alleges that he has suffered an "actual injury" in the form of lost time, money, and annoyance associated with responding to the data breach and monitoring his accounts. *See* Compl. ¶¶ 58-59, 75. But none of these alleged harms qualifies as a concrete injury for standing purposes.

As explained in *Clapper*, 568 U.S at 416, a plaintiff cannot "manufacture standing" simply by "incur[ing] certain costs as a reasonable reaction to a risk of harm." Thus, while it may have been reasonable to take some steps to mitigate the risks associated with the

[8] The Court also rejects Plaintiff's conclusory allegations that he faces a concrete harm because a second cyberattack at Leaders Life is imminent.

data breach, those actions cannot create a concrete injury where there is no imminent threat of harm. *Tsao*, 986 F.3d at 1344-1345 ("Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft."); *In re SuperValu, Inc.*, 870 F.3d at 769 (8th Cir. 2017) ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."); *Reilly*, 665 F.3d at 46 ("Appellants' alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims.").

Plaintiff also asserts that he has suffered an injury in the form of diminution in value of his personal identifying information because of the data breach. Assuming personal identifying information has a monetary value, Plaintiff fails to allege that he attempted to sell his personal information and was forced to accept a decreased price. *See Chambliss v. Carefirst, Inc*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (finding that plaintiffs had "failed to allege an injury in fact based on any diminution of the value of their personal information.").

In a final attempt to establish a concrete injury, Plaintiff asserts that he lost the benefit of his bargain with Leaders Life when he provided his personal identifying information and it was not kept secure. Compl. ¶ 68. Plaintiff has not, however, indicated that he paid any sort of premium in exchange for data security or that the data breach diminished the value of the insurance products he received in return. *See id.* (finding that

"Plaintiffs have not alleged any benefit-of-the-bargain loss that could constitute a cognizable injury in fact."); *see also Remijas*, 794 F.3d at 695 (describing plaintiff's diminution in value and benefit of the bargain theories as "dubious" and refraining from relying on these theories to support standing).

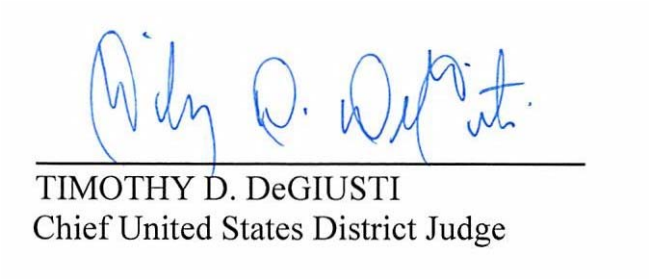
Plaintiff has failed to plausibly allege an actual, present injury that would support his damages claim or an imminent threat of future harm that would support his claim for injunctive relief. Accordingly, he lacks standing to pursue his claims.

**CONCLUSION**

The Court does not doubt that identity theft is a serious problem that involves a host of negative consequences for victims. But a data breach – even one that was intentional or involved sensitive information – does not necessarily equate to a concrete injury. In reaching this conclusion the Court does not imply that a plaintiff must always wait for identity theft or fraud to materialize before bringing suit based on a data breach, it only holds that the allegations in this case have not plausibly alleged an actual or imminent injury sufficient to establish Article III standing.

Accordingly, Defendant Leaders Life Insurance Company's Motion to Dismiss Plaintiff's First Amended Complaint [Doc. No. 11] is GRANTED, and the First Amended Complaint is DISMISSED without prejudice.

IT IS SO ORDERED this 6th day of December, 2021.



TIMOTHY D. DeGIUSTI
Chief United States District Judge